ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Τμημα **Β'**

Λυσεις Ασκησεων - Φυλλαδιο **2**

Διδασκων: Α. Μπεληγιάννης

Ιστοσελιδα Μαθηματος:
http://users.uoi.gr/abeligia/NumberTheory/NT2016/NT2016.html

Πέμπτη 27 Οκτωβρίου 2016

Άσκηση 1. *Βρείτε όλους τους φυσικούς διαιρέτες των αριθμών:*

$$140, \quad 2015, \quad 1001, \quad 9999, \quad 111111, \quad 10!, \quad \binom{30}{10}$$

Λύση. Αρκεί να βρούμε την πρωτογενή ανάλυση των παραπάνω αριθμών[1]. Έχουμε

$$140 = 2 \cdot 70 = 2 \cdot 2 \cdot 35 = 2^2 \cdot 5 \cdot 7$$

και άρα οι φυσικοί διαιρέτες του αριθμού 140 είναι:

$$\{2^a \, 5^b \, 7^c \mid \ 0 \leq a \leq 2, \ 0 \leq b, c \leq 1\}$$

δηλαδή το σύνολο $\{1, 2, 4, 5, 10, 20, 7, 14, 28, 35, 70, 140\}$.
Έχουμε:

$$2015 = 5 \cdot 13 \cdot 31$$

$$1001 = 11 \cdot 91 = 11 \cdot 7 \cdot 13$$

$$9999 = 9 \cdot 1111 = 3^2 \cdot 11 \cdot 101$$

$$111111 = 111 \cdot 1001 = 3 \cdot 37 \cdot 7 \cdot 11 \cdot 13$$

$$\begin{aligned} 10! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &= 1 \cdot 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2^3 \cdot 3^2 \cdot 2 \cdot 5 \\ &= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \end{aligned}$$

$$\begin{aligned} \binom{30}{10} &= \frac{30!}{10! \cdot (30-10)!} = \frac{30!}{10! \cdot 20!} = \frac{20! \cdot 21 \cdot 22 \cdot 23 \cdot 24 \cdot 25 \cdot 26 \cdot 27 \cdot 28 \cdot 29 \cdot 30}{20! \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10} \\ &= 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \end{aligned}$$

Από τη πρωτογενή ανάλυση των παραπάνω αριθμών βρίσκουμε όλους τους φυσικούς διαιρέτες τους, όπως ακριβώς κάναμε και με τον αριθμό 140. Για παράδειγμα οι διαιρέτες του 2015 είναι:

$$1, \quad 5, \quad 13, \quad 31, \quad 5 \cdot 13, \quad 5 \cdot 31, \quad 13 \cdot 31, \quad 5 \cdot 13 \cdot 31 = 2015$$

[1] Υπενθυμίζουμε ότι αν $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ είναι η πρωτογενής ανάλυση του φυσικού αριθμού $n > 1$, τότε ο φυσικός αριθμός d είναι διαιρέτης του n αν και μόνον αν $d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, όπου $0 \leq b_i \leq a_i$, $1 \leq i \leq k$.

■

Άσκηση 2. *Να βρεθεί η πρωτογενής ανάλυση των φυσικών αριθμών:*

$$(\alpha)\ 10^6-1, \qquad (\beta)\ 10^8-1, \qquad (\gamma)\ 2^{15}-1$$

Λύση. (α) Επειδή $10^6-1=(10^3+1)\cdot(10^3-1)$ και

$$\begin{aligned} 10^3+1 &= (10+1)\cdot(10^2-10+1) = 11\cdot 91 = 11\cdot 7\cdot 13\\ 10^3-1 &= (10-1)\cdot(10^2+10+1) = 9\cdot 111 = 3^2\cdot 3\cdot 37 = 3^3\cdot 37 \end{aligned}$$

η πρωτογενής ανάλυση του 10^6-1 είναι

$$10^6-1=3^3\cdot 7\cdot 11\cdot 13\cdot 37$$

(β) Έχουμε:

$$\begin{aligned} 10^8-1 &= (10^4)^2-1\\ &= (10^4-1)\cdot(10^4+1)\\ &= (10^2-1)\cdot(10^2+1)\cdot(10^4+1)\\ &= (10-1)\cdot(10+1)\cdot 101\cdot(10000+1)\\ &= 9\cdot 11\cdot 101\cdot 10001\\ &= 3^2\cdot 11\cdot 101\cdot 10001\\ &= 3^2\cdot 11\cdot 73\cdot 101\cdot 137 \end{aligned}$$

(γ) Έχουμε: $2^{15}-1=32768-1=32767=7\cdot 31\cdot 151.$ ■

Άσκηση 3. *Έστω $a,b,n,m\in\mathbb{N}$ έτσι ώστε: $n\geq m$. Δείξτε ότι:*

$$a^n \mid b^m \quad\Longrightarrow\quad a\mid b \qquad (*)$$

Ισχύει η παραπάνω συνεπαγωγή αν $n<m$;

Λύση. Αν $a=1$ τότε το αποτέλεσμα είναι φανερό. Επομένως υποθέτουμε $a\geq 2$. Έστω $\{p_1,\ldots,p_k\}$ το σύνολο των πρώτων αριθμών που διαιρούν τουλάχιστον έναν από τους a και b. Τότε υπάρχουν $a_i,b_i\geq 0$ ώστε

$$a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$$

και

$$b=p_1^{\beta_1}\cdots p_k^{\beta_k}.$$

Αρκεί να δείξουμε ότι $\alpha_i\leq\beta_i$ για κάθε i. Έχουμε:

$$a^n=p_1^{n\alpha_1}\cdots p_k^{n\alpha_k} \quad \& \quad b^m=p_1^{m\beta_1}\cdots p_k^{m\beta_k}$$

Επομένως

$$a^n=p_1^{n\alpha_1}\cdots p_k^{n\alpha_k}\mid b^m=p_1^{m\beta_1}\cdots p_k^{m\beta_k} \quad\Longrightarrow\quad n\alpha_i\leq m\beta_i \quad \text{για κάθε} \quad 1\leq i\leq k$$

Επειδή $n\geq m$ έπεται ότι $\alpha_i\leq\beta_i$ για κάθε $i=1,\cdots,k$ (πράγματι αν υπάρχει $i=1,2,\cdots,k$ έτσι ώστε $\alpha_i>\beta_i$, τότε η τελευταία αυτή ανισότητα πολλαπλασιασμένη με την $n\geq m$ δίνει $na_i>m\beta_i$ το οποίο είναι άτοπο). Συνεπώς $\alpha_i\leq\beta_i$ για κάθε $i=1,\cdots,k$ και άρα $a\mid b$.

Υποθέτουμε ότι $n<m$. Έστω $n=2$, $m=5$, $a=4$ και $b=2$. Τότε

$$a^n=4^2=16\mid 32=2^5=b^m$$

αλλά $a=4\nmid b=2$. Άρα αν $n<m$ η συνεπαγωγή $(*)$ δεν ισχύει. ■

Άσκηση 4. *Να δειχθεί ότι αν ένας περιττός πρώτος αριθμός p είναι ίσος με το άθροισμα δύο τετραγώνων, τότε ο p είναι της μορφής $4k+1$.*[2]

Λύση. Κάθε θετικός ακέραιος αριθμός έχει μια από τις παρακάτω μορφές $4k$, $4k+1$, $4k+2$, $4k+3$. Επειδή ο p είναι πρώτος, έπεται ότι ο p θα έχει μια από τις μορφές $4k+1$, $4k+3$.

Υποθέτουμε ότι υπάρχουν ακέραιοι a, b έτσι ώστε $p = a^2 + b^2$.

(1) Αν οι a, b είναι και οι δύο άρτιοι ή είναι και οι δύο περιττοί, τότε προφανώς ο αριθμός $p = a^2+b^2$ θα είναι άρτιος και επειδή ο p είναι πρώτος, θα έχουμε ότι $p = 2 = a^2 + b^2$. Αυτό είναι άτοπο διότι από την υπόθεση ο p είναι περιττός.

(2) Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι ο a είναι άρτιος και ο b είναι περιττός. Τότε $a = 2\lambda$ και $b = 2\mu + 1$ για κάποιους ακέραιους λ, μ. Τότε θα έχουμε

$$p = a^2 + b^2c = (2\lambda)^2 + (2\mu+1)^2 = 4\lambda^2 + 4\mu^2 + 4\mu + 1 = 4(\lambda^2 + \mu^2 + \mu) + 1$$

και άρα ο p είναι της μορφής $4k+1$. ■

Στην επίλυση της επόμενης άσκησης χρησιμοποιούμε τις ακόλουθες γνωστές ταυτότητες, όπου $n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1})$$

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots + ab^{n-2} - b^{n-1}), \qquad n: \text{ περιττός}$$

Άσκηση 5. *Έστω $a, n > 1$ είναι δύο θετικοί ακέραιοι.*

(1) *Να δειχθεί ότι αν ο αριθμός $a^n + 1$ είναι πρώτος, τότε ο a είναι άρτιος και υπάρχει $m \geq 1$ έτσι ώστε: $n = 2^m$.*

(2) *Να δειχθεί ότι αν ο αριθμός $a^n - 1$ είναι πρώτος, τότε $a = 2$ και ο αριθμός n είναι πρώτος.*

Λύση. **1.** Υποθέτουμε ότι ο αριθμός $a^n + 1$ είναι πρώτος. Αν ο a είναι περιττός, τότε ο αριθμός a^n είναι περιττός και επομένως ο αριθμός $a^n + 1$ είναι άρτιος. Επειδή ο $a^n + 1$ είναι πρώτος έπεται ότι $a^n + 1 = 2$ και επομένως $a^n = 1$. Αυτό είναι άτοπο διότι $a > 1$. Επομένως ο a είναι άρτιος.

Υποθέτουμε ότι ο θετικός ακέραιος n δεν είναι της μορφής 2^m για κάποιο $m \geq 1$. Τότε ο n θα έχει έναν περιττό πρώτο διαιρέτη p. Αν $n = p$, τότε θα έχουμε

$$a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + a^{n-3} - \cdots + a - 1)$$

Επειδή ο αριθμός $a^n + 1$ είναι πρώτος, έπεται ότι είτε $a + 1 = 1$ είτε $a + 1 = a^n + 1$. Ισοδύναμα, είτε $a = 0$ είτε $a^n = a$. Επειδή $a, n > 1$ και στις δύο περιπτώσεις καταλήγουμε σε άτοπο.

Αν $p < n$, τότε θέτοντας $k = \frac{n}{p}$ θα έχουμε ότι $k > 1$ και τότε

$$a^n + 1 = (a^{\frac{n}{p}})^p + 1 = (a^k)^p + 1 = (a^k + 1)((a^k)^{p-1} - (a^k)^{p-2} + (a^k)^{p-3} - \cdots + a^k - 1)$$

Επειδή ο αριθμός $a^n + 1$ είναι πρώτος, έπεται ότι είτε $a^k + 1 = 1$ είτε $a^k + 1 = a^n + 1$. Ισοδύναμα, είτε $a^k = 0$ είτε $a^k = a^n$. Επειδή $a, n > 1$ και $k < n$ και στις δύο περιπτώσεις καταλήγουμε προφανώς σε άτοπο.

Επομένως ο αριθμός n δεν έχει περιττό πρώτο διαιρέτη, δηλαδή ο μόνος πρώτος διαιρέτης του είναι ο 2. Αυτό σημαίνει ότι $n = 2^m$ για κάποιο $m \geq 1$.

---

[2] Σύμφωνα με ένα Θεώρημα του Fermat του οποίου η απόδειξη ξεφεύγει από τα πλαίσια του μαθήματος, αντίστροφα, κάθε πρώτος αριθμός της μορφής $4k+1$ είναι άθροισμα δύο τετραγώνων.

2. Υποθέτουμε ότι ο αριθμός a^n+1 είναι πρώτος. Επειδή

$$a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots+a+1)$$

έπεται ότι είτε $a-1=1$ είτε $a^{n-1}=a-1$. Αν $a-1=1$, τότε $a=2$. Αν $a^n-1=a-1$, τότε $a^n=a$, το οποίο είναι άτοπο διότι $a,n>1$. Επομένως $a=2$.

Υποθέτουμε ότι n δεν είναι πρώτος. Τότε μπορούμε να γράψουμε

$$n=rs,\quad 1<r,s<n$$

και θα έχουμε

$$2^n-1=2^{rs}-1=(2^r)^s-1=(2^r-1)((2^r)^{s-1}+(2^r)^{s-2}+\cdots+2^r+1$$

Επειδή ο αριθμός 2^n-1 είναι πρώτος, έπεται ότι είτε $2^r-1=1$ είτε $2^r-1=2^n-1$. Αν $2^r-1=1$, τότε $2^r=2$ και αυτό είναι άτοπο διότι $r>1$. Αν $2^r-1=2^n-1$, τότε $2^r=2^n$, και αυτό είναι επίσης άτοπο διότι $r<n$.

Στο άτοπο οδηγηθήκαμε υποθέτοντας ότι ο n είναι σύνθετος. Άρα ο n είναι πρώτος. ■

Άσκηση 6. *Έστω p ένας πρώτος αριθμός.*

1. *Αν k είναι ένας θετικός ακέραιος και $k<p$, δείξτε ότι: $p \mid \binom{p}{k}$.*

2. *Αν n είναι ένας θετικός ακέραιος και $n<p\leq 2n$, δείξτε ότι: $p \mid \binom{2n}{n}$.*

Λύση. **1.** Επειδή ο αριθμός $\binom{p}{k}$ είναι θετικός ακέραιος, μπορούμε να θέσουμε

$$\binom{p}{k}=\frac{p!}{k!(p-k)!}=r,\qquad \text{όπου}\quad r\in\mathbb{N}$$

και επομένως $p!=rk!(p-k)!$. Επειδή $p \mid p!$, θα έχουμε $p \mid rk!(p-k)!$. Επειδή ο p είναι πρώτος, από το Λήμμα του Ευκλείδη[3], έπεται ότι ο p διαιρεί κάποιον από τους $k!,\ (p-k)!,\ r$. Όμως αν $p \mid k!$, τότε πάλι από το Λήμμα του Ευκλείδη θα έχουμε $p \mid l$ για κάποιο $l\leq k$, και ιδιαίτερα $p\leq l\leq k$. Αυτό είναι άτοπο διότι $k<p$. Αν $p \mid (p-k)!$, τότε καταλήγουμε στο άτοπο ότι $p \mid l$, και ιδιαίτερα $p\leq l$, για κάποιο $l\leq p-k<p$. Επομένως θα έχουμε $p \mid r$ και άρα $p \mid \binom{p}{k}$.

2. Επειδή ο αριθμός $\binom{2n}{n}$ είναι θετικός ακέραιος, μπορούμε να θέσουμε

$$\binom{2n}{n}=\frac{(2n)!}{n!n!}=\frac{(2n)!}{(n!)^2}=r,\qquad \text{όπου}\quad r\in\mathbb{N}$$

και επομένως $(2n)!=r(n!)^2$. Επειδή $p\leq 2n$, έπεται προφανώς ότι $p \mid (2n)!$, και άρα $p \mid r(n!)^2$. Επειδή ο p είναι πρώτος, τότε από το Λήμμα του Ευκλείδη, έπεται ότι είτε ο p διαιρεί κάποιον από τους $n!,\ r$. Όμως αν $p \mid n!$, τότε πάλι από το Λήμμα του Ευκλείδη θα έχουμε $p \mid l$ για κάποιο $l\leq n$, και ιδιαίτερα $p\leq l\leq n$. Αυτό είναι άτοπο διότι $n<p$. Επομένως $p \mid r$ και άρα $p \mid \binom{2n}{n}$. ■

Άσκηση 7. *Να βρεθούν όλες οι θετικές ακέραιες λύσεις της εξίσωσης*

$$m^n=n^m$$

δηλαδή να βρεθούν όλα τα ζεύγη θετικών ακεραίων αριθμών (n,m) τα οποία ικανοποιούν την παραπάνω εξίσωση.

[3] Λημμα του Ευκλειδη: *Αν p είναι ένας πρώτος αριθμός και $a,b\in\mathbb{Z}$, τότε: $p \mid ab \implies p \mid a$ ή $p \mid b$.*

Λύση. Αν $n = 1$ τότε φανερά πρέπει $m = 1$. Ομοίως αν $m = 1$ τότε πρέπει $n = 1$.

Επομένως υποθέτουμε $n, m \geq 2$.

Επειδή $m^n = n^m$ τότε έπεται άμεσα από τη θεωρία, παραδείγματος χάριν με χρήση του Λήμματος του Ευκλείδη, ότι οι αριθμοί m και n έχουν τους ίδιους πρώτους διαιρέτες. Έστω

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \& \quad n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

οι πρωτογενείς αναλύσεις των αριθμών m και n αντίστοιχα. Τότε χρησιμοποιώντας την μοναδικότητα της ανάλυσης σε πρώτους παράγοντες, θα έχουμε:

$$m^n = n^m \implies p_1^{na_1} p_2^{na_2} \cdots p_k^{na_k} = p_1^{mb_1} p_2^{mb_2} \cdots p_k^{mb_k} \implies a_i n = b_i m, \quad \forall i = 1, 2, \cdots, k$$

Προφανώς αν $n = m$ τότε η εξίσωση $m^n = n^m$ ικανοποιείται.

Υποθέτουμε λοιπόν ότι $m \neq n$ και έστω $n > m$. Επειδή $a_i n = b_i m$ και $n > m$ έπεται ότι $a_i < b_i$ για κάθε $i = 1, 2, \cdots k$. Αυτό όμως σημαίνει ότι $m \mid n$ διότι μπορούμε να γράψουμε

$$n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} = p_1^{b_1 - a_1} p_2^{b_2 - a_2} \cdots p_k^{b_k - a_k} \cdot p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = d \cdot m, \quad \text{όπου} \quad d = p_1^{a_1 - b_1} p_2^{a_2 - b_2} \cdots p_k^{a_k - b_k}$$

Άρα

$$m \mid n \implies n = dm \implies m^{dm} = (dm)^m \implies m^d = dm \implies m^{d-1} = d$$

Επειδή $n > m$ έχουμε ότι $d > 1$. Διακρίνουμε τις περιπτωσεις:

(1) Αν $d = 2$ τότε θα έχουμε $m^{2-1} = 2$ και άρα $m = 2$ και $n = dm = 4$.

(2) Αν $d > 2$, τότε επειδή $m \geq 2$, θα έχουμε: $m^{d-1} \geq 2^{d-1}$.

Δείχνουμε με χρήση της Αρχής Μαθηματικής Επαγωγής ότι: $2^{d-1} > d$, $\forall d \geq 3$.

Πράγματι η ανισότητα ισχύει για $d = 3$, διότι $2^{3-1} = 2^2 = 4 > 3$. Έστω $d > 3$ και υποθέτουμε ότι $2^{d-1} > d$. Τότε $2^d = 2 \cdot 2^{d-1} > 2d > 1 + d$. Άρα απο την Αρχή Μαθηματικής Επαγωγής η ανισότητα $2^{d-1} > d$ ισχύει για κάθε $d \geq 3$.

Επομένως θα έχουμε $m^{d-1} \geq 2^{d-1} > d$ το οποίο είναι άτοπο.

Άρα οι μόνες λύσεις με $n > m$ είναι $m = 2$ και $n = 2d = 2 \cdot 2 = 4$.

Επομένως όλες οι λύσεις της εξίσωσης $m^n = n^m$ είναι οι ακόλουθες:

$$\begin{cases} m = 2 \quad \text{και} \quad n = 4 \\ \\ n = 2 \quad \text{και} \quad m = 4 \\ \\ n = m \end{cases}$$

■

Άσκηση 8. *Έστω n ένας φυσικός αριθμός.*

1. *Αν ο n είναι περιττός, δείξτε ότι:*

$$\frac{n(n+1)}{2} \mid n!$$

2. *Αν $n > 1$, δείξτε ότι:*

$$\frac{n(n+1)}{2} \nmid n! \quad \implies \quad n+1 : \textit{πρώτος}$$

Ισχύει η αντίστροφη συνεπαγωγή; Δηλαδή αν ο αριθμός $n+1$ είναι πρώτος, ισχύει ότι $\frac{n(n+1)}{2} \nmid n!$;

Λύση. **1.** Επειδή ο n είναι περιττός, θα έχουμε $n = 2k+1$, για κάποιο $k \geq 0$, και τότε $n+1 = 2(k+1)$. Επομένως

$$\frac{n(n+1)}{2} = \frac{(2k+1)2(k+1)}{2} = (k+1)(2k+1) = (k+1)n$$

Επειδή $k + 1 < n$, έπεται ότι $n! = 1 \cdot 2 \cdot \cdots (k+1) \cdot \cdots \cdot n$ και επομένως $\frac{n(n+1)}{2} = (k+1)n \mid n!$

2. Ο n είναι άρτιος διότι αν ήταν περιττός, τότε από το **1.** θα είχαμε ότι $\frac{n(n+1)}{2} \mid n!$ το οποίο είναι άτοπο από την υπόθεση. Έτσι $n = 2k$ για κάποιο $k \geq 1$. Θα δείξουμε ότι ο περιττός αριθμός $n+1$ είναι πρώτος.

Έστω ότι ο $n+1 = 2k+1$ είναι σύνθετος. Τότε $n+1 = a \cdot b$ για κάποιους θετικούς ακέραιους a, b με $1 < a, b < n = 2k+1$. Τότε:

$$\frac{n(n+1)}{2} \nmid n! \implies \frac{2kab}{2} \nmid (2k)! \implies k \cdot a \cdot b \nmid (2k)!$$

Αυτό είναι άτοπο διότι $k \geq 1$ και $1 < a, b \leq 2k$. Επομένως ο $n+1$ είναι πρώτος αριθμός.

Αντίστροφα, έστω ότι ο αριθμός $n+1$ είναι πρώτος.

Αν $n+1 = 2$, τότε $n = 1$, το οποίο είναι άτοπο διότι $n > 1$. Άρα $n+1 > 2$, και τότε ο $n+1$ είναι περιττός. Αυτο σημαίνει ότι ο n είναι άρτιος, δηλαδή $\frac{n}{2} = k \in \mathbb{N}$. Επομένως $\frac{n(n+1)}{2} = k(n+1)$ και άρα αν $\frac{n(n+1)}{2} \mid n!$, τότε θα έχουμε $k(n+1) \mid n!$. Επειδή προφανώς $n+1 \mid k(n+1)$, έπεται ότι $n+1 \mid n!$ και επειδή ο αριθμός $n+1$ είναι πρώτος, από το Λήμμα του Ευκλείδη θα έχουμε ότι $n+1 \mid l$, και ιδιάιτερα $n+1 \leq l$, για κάποιο $l \leq n$. Φυσικά αυτό είναι άτοπο και επομένως καταλήγουμε ότι $\frac{n(n+1)}{2} \nmid n!$, δηλαδή η αντίστροφη συνεπαγωγή ισχύει. ■

Άσκηση 9. *Ένας εκδοτικός οίκος από τις πωλήσεις ενός βιβλίου είχε έσοδα* $375.961€$. *Μπορείτε να εκτιμήσετε πόσα βιβλία πούλησε ο εκδοτικός οίκος αν η τιμή του βιβλίου είναι ακέραιος και πάνω από ένα ευρώ;*

Λύση. Έστω m η τιμή του βιβλίου και n ο αριθμός των βιβλίων που πουλήθηκαν. Τότε προφανώς θα έχουμε:

$$375961 = m \cdot n$$

Επομένως οι αριθμοί είναι διαιρέτες του 375961.

Η πρωτογενής ανάλυση του αριθμού 375961 είναι

$$375961 = 79 \cdot 4759$$

και επομένως οι διαιρέτες του 375961, εκτός των 1 και 375961, είναι οι αριθμοί 79 και 4759. Άρα η πιθανότερη εκδοχή είναι ότι $n = 4759$, και $m = 79$.

Επομένως το πιθανότερο είναι ότι ο εκδοτικός οίκος πούλησε 4759 βιβλία στη τιμή των $79€$. ■

Άσκηση 10. *Υπενθυμίζουμε ότι ένας πραγματικός αριθμός a καλείται άρρητος αν $a \in \mathbb{R} \setminus \mathbb{Q}$, δηλαδή δεν μπορεί να εκφρασθεί στη μορφή $\frac{n}{m}$, $n, m \in \mathbb{Z}$, $m \neq 0$.*

1. *Να δειχθεί ότι ο $\sqrt{2}$ είναι άρρητος.*
2. *Να δειχθεί ότι, για κάθε πρώτο p, ο $\sqrt{p}$ είναι άρρητος.*
3. *Να δείξετε ότι αν ο φυσικός αριθμός n δεν είναι τετράγωνο ακεραίου, τότε ο αριθμός $\sqrt{n}$ είναι άρρητος.*
4. *Αν $n, m \in \mathbb{N}$ όπου $n, m > 1$, και ο αριθμός $\sqrt[n]{m}$ είναι ρητός, τότε να δείξετε ότι ο αριθμός $\sqrt[n]{m}$ είναι ακέραιος.*

Λύση. **1.** Υποθέτουμε αντίθετα ότι $\sqrt{2} \in \mathbb{Q}$. Άρα $\sqrt{2} = \frac{a}{b}$ όπου $a, b \in \mathbb{Z}, b \neq 0$ και χωρίς βλάβη της γενικότητας υποθέτουμε ότι οι a, b δεν έχουν κοινό παράγοντα. Τότε

$$\sqrt{2} = \frac{a}{b} \implies a^2 = 2b^2 \implies 2 \mid a^2 \implies 2 \mid a \tag{1}$$

Αφού το 2 διαιρεί τον αριθμό a τότε $a = 2c$ και επομένως έχουμε

$$a^2 = 4c^2 \implies 4c^2 = 2b^2 \implies 2c^2 = b^2 \implies 2 \mid b^2 \implies 2 \mid b \tag{2}$$

Από τις σχέσεις (1) και (2) έπεται ότι το 2 είναι κοινός παράγοντας των a, b. Αυτό όμως είναι άτοπο και άρα $\sqrt{2} \notin \mathbb{Q}$.

2. Η απόδειξη είναι παρόμοια με την απόδειξη του **1**: υποθέτουμε αντίθετα ότι $\sqrt{p} \in \mathbb{Q}$. Άρα $\sqrt{p} = \frac{a}{b}$ όπου $a, b \in \mathbb{Z}, b \neq 0$ και χωρίς βλάβη της γενικότητας υποθέτουμε ότι οι a, b δεν έχουν κοινό παράγοντα. Τότε, χρησιμοποιώντας ότι ο p είναι πρώτος, Θα έχουμε

$$\sqrt{p} = \frac{a}{b} \implies a^2 = pb^2 \implies p \mid a^2 \implies p \mid a \tag{3}$$

Επειδή το p διαιρεί τον αριθμό a τότε $a = pc$ και επομένως χρησιμοποιώντας ότι ο p είναι πρώτος, Θα έχουμε

$$a^2 = p^2c^2 \implies p^2c^2 = pb^2 \implies pc^2 = b^2 \implies p \mid b^2 \implies p \mid b \tag{4}$$

Από τις σχέσεις (3) και (4) έπεται ότι το p είναι κοινός παράγοντας των a, b. Αυτό όμως είναι άτοπο από την υπόθεση και άρα $\sqrt{2} \notin \mathbb{Q}$.

3. Έστω ότι $\sqrt{n} \in \mathbb{Q}$, δηλαδή $\sqrt{n} = \frac{a}{b}$ με $a, b \in \mathbb{Z}, b \neq 0$ και χωρίς βλάβη της γενικότητας υποθέτουμε ότι οι a, b δεν έχουν κοινό παράγοντα. Τότε $a^2 = nb^2$ και από την υπόθεση μας το n δεν είναι τετράγωνο ακεραίου. Άρα υπάρχει πρώτος αριθμός p έτσι ώστε

$$p \mid n \quad \text{και} \quad p^2 \nmid n$$

Επομένως μπορούμε να γράψουμε

$$n = pn' \quad \text{όπου} \quad p \nmid n'$$

Τότε

$$\begin{cases} p \mid n \\ \\ n \mid a^2 \end{cases} \implies p \mid a^2 \implies p \mid a$$

Άρα $a = pc$ και τότε έχουμε

$$a^2 = p^2c^2 = nb^2 = pn'b^2 \implies pc^2 = n'b^2 \implies \begin{cases} p \mid n'b^2 \\ \\ p \nmid n' \end{cases} \implies p \mid b^2 \implies p \mid b$$

Τότε ο πρώτος p είναι κοινός παράγοντας των a και b και επομένως έχουμε καταλήξει σε άτοπο.
Άρα $\sqrt{n} \notin \mathbb{Q}$.

4. Έχουμε $\sqrt[n]{m} = \frac{a}{b}$ και υποθέτουμε ότι οι αριθμοί a, b δεν έχουν κοινό παράγοντα. Έστω ότι $b > 1$. Τότε υπάρχει πρώτος $p \mid b$ έτσι ώστε

$$\sqrt[n]{m} = \frac{a}{b} \implies \begin{cases} a^n = mb^n \\ \\ p \mid b \end{cases} \implies p \mid a^n \implies p \mid a$$

Τότε ο πρώτος p είναι κοινός παράγοντας των a και b και επομένως έχουμε καταλήξει σε άτοπο.
Συνεπώς $b = 1$ και επομένως $\sqrt[n]{m} \in \mathbb{Z}$. ■

Άσκηση 11. (1) *Να δείξετε ότι ο φυσικός αριθμός n είναι τέλειο τετράγωνο αν και μόνον αν οι δυνάμεις στην πρωτογενή ανάλυση του n είναι άρτιοι αριθμοί.*

(2) *Έστω $n \geq 2$ και*

$$a = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

η πρωτογενής ανάλυση του φυσικού αριθμού a. Δείξτε ότι η n-στή ρίζα του a είναι ρητός αριθμός αν και μόνο αν το n διαιρεί το a_i για κάθε $i = 1, 2, \cdots, m$:

$$\sqrt[n]{a} \in \mathbb{Q} \iff n \mid a_i, \quad 1 \leq i \leq m$$

Λύση. (1) Θα δείξουμε ότι ο αριθμός $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ είναι τέλειο τετράγωνο αν και μόνο αν τα a_i είναι άρτιοι αριθμοί για κάθε $1 \leq i \leq k$.

Αν για κάθε $1 \leq i \leq k$ οι αριθμοί a_i είναι άρτιοι, τότε $a_i = 2b_i$ και άρα

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = p_1^{2b_1} p_2^{2b_2} \cdots p_k^{2b_k} = (p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k})^2$$

Συνεπώς ο αριθμός n είναι τέλειο τετράγωνο.

Έστω $n = m^2$ και $m = p_1^{b_1} \cdots p_k^{b_k}$ η πρωτογενής ανάλυση του m. Τότε

$$n = m^2 = p_1^{2b_1} \cdots p_k^{2b_k} \implies p_1^{a_1} \cdots p_k^{a_k} = p_1^{2b_1} \cdots p_k^{2b_k}$$

και λόγω μοναδικότητας της παραγοντοποίησης έπεται ότι $a_i = 2b_i$ για κάθε $1 \leq i \leq k$.

(2) Έστω ότι $\sqrt[n]{a} \in \mathbb{Q}$. Τότε από το τρίτο ερώτημα της Άσκησης 10 έπεται ότι $\sqrt[n]{a} \in \mathbb{Z}$. Έστω

$$\sqrt[n]{a} = p_1^{k_1} \cdots p_m^{k_m}$$

η πρωτογενής ανάλυση του $\sqrt[n]{a}$. Τότε

$$a = (p_1^{k_1} \cdots p_m^{k_m})^n \implies a = p_1^{a_1} \cdots p_m^{a_m} = p_1^{nk_1} \cdots p_m^{nk_m} \implies a_i = nk_i$$

Συνεπώς $n \mid a_i$ για κάθε $1 \leq i \leq m$.

Αντίστροφα, έστω $a = p_1^{a_1} \cdots p_m^{a_m}$ η πρωτογενής ανάλυση του a και έστω $n \mid a_i$ για κάθε $1 \leq i \leq m$. Άρα $a_i = nk_i$ και τότε

$$a = p_1^{a_1} \cdots p_m^{a_m} = p_1^{nk_1} \cdots p_m^{nk_m} = (p_1^{k_1} \cdots p_m^{k_m})^n$$

Επομένως έχουμε: $\sqrt[n]{a} = p_1^{k_1} \cdots p_m^{k_m} \in \mathbb{Z} \subseteq \mathbb{Q}$. ■

Άσκηση 12. *Έστω $a > 1$ ένας φυσικός αριθμός.*

1. *Δείξτε ότι ο αριθμός*

$$\mathsf{min}\big\{k \in \mathbb{N} \mid k \neq 1 \ \ \& \ \ k \mid a\big\}$$

είναι πρώτος.

2. *Αν ο αριθμός a είναι σύνθετος, δείξτε ότι:*

$$\mathsf{min}\big\{k \in \mathbb{N} \mid k \neq 1 \ \ \& \ \ k \mid a\big\} \ \leq \ \sqrt{a}$$

Λύση. Θεωρούμε το σύνολο

$$X = \big\{k \in \mathbb{N} \mid k \neq 1 \ \ \& \ \ k \mid a\big\} \ \subseteq \ \mathbb{N}$$

Επειδή $a > 1$, το σύνολο X είναι μη-κενό διότι περιέχει το a. Επομένως από την Αρχή Καλής Διάταξης το σύνολο X έχει ελάχιστο στοιχείο, έστω:

$$p = \mathsf{min}X$$

1. Θα δείξουμε ότι ο p είναι πρώτος. Επειδή $p > 1$, ο p έχει έναν πρώτο διαιρέτη q. Επειδή $q \mid p$ και $p \mid a$, έπεται ότι $q \mid a$ και άρα επειδή $q > 1$ (επειδή ο q είναι πρώτος), έπεται ότι $q \in X$. Επειδή $q \mid p = \mathsf{min}X$, έπεται ότι $q \leq p$ και επομένως $q = p$, δηλαδή ο p είναι πρώτος.

2. Αν ο a είναι σύνθετος, τότε προφανώς $p \neq a$ και επειδή $p \mid a$, έπεται ότι $a = pb$, όπου $1 < b < a$. Επειδή $b > 1$, ο b έχει έναν πρώτο διαιρέτη q. Ο q είναι προφανώς και διαιρέτης του a, και επομένως $p \leq q \leq b$ διότι ο q είναοι ο μικρότερος (πρώτος) διαιρλετης του a. Έτσι θα έχουμε

$$a = pb \geq pp = p^2 \quad \implies \quad p \leq \sqrt{a}$$ ■

Άσκηση 13. *Να δειχθεί ότι για κάθε θετικό ακέραιο $n > 2$, υπάρχει ένας πρώτος αριθμός p έτσι ώστε:*

$$n \ < \ p \ < \ n!$$

Λύση. Επειδή $n > 2$, έπεται ότι $n! > 2$ και άρα $n! - 1 > 1$. Τότε όπως γνωρίζουμε ο αριθμός $n! - 1$ έχει έναν πρώτο διαιρέτη p, και τότε $p \leq n! - 1 < n!$.

Αν $p \leq n$, τότε προφανώς θα έχουμε ότι $p \mid n!$ και επομένως, επειδή $p \mid n! - 1$, έπεται ότι $p \mid 1$ το οποίο είναι άτοπο. Άρα $p > n$ και άρα τελικά θα έχουμε $n < p < n!$. ■

Άσκηση 14. *Να δειχθεί ότι αν οι αριθμοί p και $p + 2$, όπου $p > 3$, είναι πρώτοι*[4]*, τότε*

$$6 \mid p + 1$$

Λύση. Επειδή ο p είναι μεγαλύτερος του 3 έπεται ότι ο p είναι περιττός και επομένως ο $p + 1$ είναι άρτιος. Αυτό σημαίνει ότι $2 \mid p + 1$.

Ο αριθμός $p + 1$ έχει μια από τις παρακάτω μορφές: $3k$, $3k + 1$, $3k + 2$.

(1) Αν $p + 1 = 3k + 1$, τότε $p = 3k$ και και αυτό είναι άτοπο διότι ο p είναι πρώτος και $p > 3$.

(2) Αν $p + 1 = 3k + 2$, τότε $p = 3k + 1$ και άρα $p + 2 = 3k + 1 + 2 = 3k + 3 = 3(k + 1)$ το οποίο είναι άτοπο διότι ο $p + 2$ είναι πρώτος και $p + 2 > 3 + 2 = 5$.

Άρα μένει η περίπτωση $p + 1 = 3k$ και επομένως $3 \mid p + 1$. Επειδή επίσης ισχύει ότι $2 \mid p + 1$ και οι 2 και 3 είναι πρώτοι μεταξύ τους, έπεται ότι $6 \mid p + 1$. ■

Άσκηση 15. *Να βρεθούν όλοι οι φυσικοί αριθμοί οι οποίοι έχουν ακριβώς (α) 3, και (β) 4, θετικούς διαιρέτες.*

Λύση. (α) Έστω $\alpha \in \mathbb{N}$ με ακριβώς 3 θετικούς διαιρέτες. Επειδή $1, \alpha \mid \alpha$ έπεται ότι ο α έχει ακριβώς έναν διαιρέτη $d \mid \alpha$ με $d \neq 1$ και $d \neq \alpha$. Έστω $\alpha = p_1^{a_1} \cdots p_n^{a_n}$ η πρωτογενής ανάλυση του αριθμού α. Αν $n \geq 2$ τότε οι αριθμοί $1, p_1, p_2, p_1 p_2 \mid \alpha$, που είναι άτοπο. Άρα $n = 1$, δηλαδή $\alpha = p_1^{a_1}$. Αν $a_1 \geq 3$ τότε $1, p, p^2, p^3 \mid \alpha$ που είναι άτοπο διότι ο αριθμός α έχει ακριβώς 3 διαιρέτες. Επομένως $\alpha = p^2$, όπου p πρώτος αριθμός.

(β) Έστω $\alpha \in \mathbb{N}$ με ακριβώς 4 θετικούς διαιρέτες και έστω $\alpha = p_1^{a_1} \cdots p_n^{a_n}$ η πρωτογενής ανάλυση του αριθμού α. Διακρίνουμε τις περιπτώσεις:

(1) Αν $n = 1$ τότε $\alpha = p^k$. Φανερά για την τιμή $k = 3$ και μόνο για αυτήν ο αριθμός $\alpha = p^3$ έχει ακριβώς 4 διαιρέτες: $1, p, p^2, p^3$.

(2) Αν $n = 2$ τότε $\alpha = p_1^{a_1} p_2^{a_2}$. Άρα μόνο για $a_1 = a_2 = 1$ ο αριθμός α έχει ακριβώς 4 διαιρέτες: $1, p_1, p_2, p_1 p_2$.

(3) Αν $n \geq 3$ τότε επειδή οι $1, p_1, p_2, p_3, p_1 p_2$ είναι διαιρέτες του α ο αριθμός α έχει περισσότερους από 4 διαιρέτες. ■

Άσκηση 16. *Ένα μη-σταθερό πολυώνυμο $f(t) \in \mathbb{Z}[t]$ με ακέραιους συντελεστές καλείται ανάγωγο αν δεν υπάρχουν πολυώνυμα $g(t), h(t) \in \mathbb{Z}[t]$ μικρότερου βαθμού με $f(t) = g(t)h(t)$.*

Δείξτε το ακόλουθο Κριτηριο Eisenstein*: Θεωρούμε ένα πολυώνυμο με ακέραιους συντελεστές*

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n, \qquad n > 0, \quad a_i \in \mathbb{Z}, \ \ 0 \leq i \leq n \quad \textit{και} \quad a_n \neq 0$$

και έστω p ένας πρώτος αριθμός. Τότε:

$$p \mid a_0, \ p \mid a_1, \ \cdots, \ p \mid a_{n-1} \quad \& \quad p \nmid a_n \quad \& \quad p^2 \nmid a_0 \quad \Longrightarrow \quad f(t): \ \textit{ανάγωγο}$$

Εφαρμογη*: Δείξτε ότι τα πολυώνυμα $g_1(t) = t^4 - 6t^3 + 24t^2 - 30t + 14$, $g_2(t) = t^7 + 48t - 24$, $g_3(t) = t^5 + 5t + 5$, και $g_4(t) = t^n - p$, όπου p είναι ένας πρώτος αριθμός και $n > 1$, είναι ανάγωγα υπεράνω του $\mathbb{Q}$. Είναι το πολυώνυμο $t^4 + 4$ και ανάγωγο υπεράνω του $\mathbb{Q}$;*

[4] Δηλαδή οι p και $q = p + 2$ είναι *δίδυμοι πρώτοι*.

Λύση. Έστω ότι το πολυώνυμο $f(t)$ δεν είναι ανάγωγο. Άρα $f(t) = g(t)h(t)$ όπου $g(t) = b_0 + b_1 t + \cdots + b_s t^s \in \mathbb{Z}[t]$, $h(t) = c_0 + c_1 t + \cdots + c_r t^r \in \mathbb{Z}[t]$ και $s \geq 1$, $r \geq 1$. Τότε

$$a_0 = b_0 c_0, \quad a_1 = b_0 c_1 + b_1 c_0, \cdots, \quad a_i = b_0 c_i + b_1 c_{i-1} + \cdots + b_i c_0$$

όπου $0 \leq i \leq n$. Αφού $p \mid a_0$ και $a_0 = b_0 c_0$ έπεται ότι $p \mid b_0$ ή $p \mid c_0$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $p \mid b_0$. Τότε $p \nmid c_0$, διότι αν $p \mid c_0$, θα είχαμε ότι $p^2 \mid b_0 c_0 = a_0$ το οποίο είναι άτοπο. Αν $p \mid b_s$ τότε

$$p \mid b_s c_r \implies p \mid a_n$$

που είναι άτοπο. Άρα $p \nmid b_s$. Επομένως υπάρχει ένα $i \leq s$ έτσι ώστε $p \mid b_0, b_1, \cdots b_{i-1}$ και $p \nmid b_i$. Όμως $a_i = b_0 c_i + b_1 c_{i-1} + \cdots + b_{i-1} c_1 + b_i c_0$ και

$$\begin{cases} p \mid a_i \\ \\ p \mid b_0 c_i + \cdots + b_{i-1} c_1 \end{cases} \implies \begin{cases} p \mid b_i c_0 \\ \\ p \nmid c_0 \end{cases} \implies p \mid b_i$$

που είναι άτοπο. Συνεπώς το πολυώνυμο $f(t)$ είναι ανάγωγο.

Εφαρμογη: Επιλέγοντας, $p = 2$ για το $g_1(t)$, $p = 3$ για το $g_2(t)$, $p = 5$ για το $g_3(t)$, και $p = p$, για το $g_4(t)$, από το Κριτήριο Eisenstein βλέπουμε ότι τα πολυώνυμα $g_i(t)$, $1 \leq i \leq 4$, είναι ανάγωγα υπεράνω του $\mathbb{Q}$.

Αντίθετα το πολυώνυμο $t^4 + 4$, για το οποίο δεν μπορεί να εφαρμοσθεί το Κριτήριο Eisenstein, δεν είναι ανάγωγο διότι:

$$t^4 + 4 = \left(t^2 - 2t + 2\right) \cdot \left(t^2 + 2t + 2\right)$$

■

Άσκηση 17. *Θεωρούμε ένα πολυώνυμο με ακέραιους συντελεστές*

$$f(t) = t^n + c_{n-1} t^{n-1} + \cdots c_1 t + c_0,$$

Αν ρ είναι μια πραγματική ρίζα του $f(t)$, να δείξετε ότι: είτε ο ρ είναι ακέραιος ή ο ρ είναι άρρητος.

Λύση. Έστω $p = \frac{a}{b} \in \mathbb{Q}$ μια ρίζα του $f(t)$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι οι a, b δεν έχουν κανένα κοινό παράγοντα.

Άρα

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1 \frac{a}{b} + c_0 = 0$$

Πολλαπλασιάζοντας της παραπάνω σχέση με b^n θα έχουμε

$$\begin{aligned} a^n + c_{n-1} a^{n-1} b + \cdots + c_1 a b^{n-1} + c_0 b^n = 0 &\implies a^n = b(-c_{n-1} a^{n-1} - \cdots - c_1 a b^{n-2} - c_0 b^{n-1}) \\ &\implies b \mid a^n \end{aligned}$$

Υποθέτουμε ότι $b \neq \pm 1$. Τότε ο b έχει ένα πρώτο διαιρέτη q και άρα

$$\begin{cases} q \mid b \\ \\ b \mid a^n \end{cases} \implies q \mid a^n \implies q \mid a$$

Συνεπώς οι a, b έχουν ένα κοινό πρώτο διαιρέτη που είναι άτοπο.

Άρα $b = \pm 1$ και έτσι έχουμε το ζητούμενο. ■

Άσκηση 18. *Δείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής:* (α) $3k + 2$ *και* (β) $4k + 3$.

Λύση. (α) Υποθέτουμε ότι υπάρχει πεπερασμένο πλήθος πρώτων της μορφής $3k+2$, και έστω ότι όλοι οι πρώτοι της μορφής $3k+2$ είναι οι $p_1, p_2, \cdots, p_n$. Θεωρούμε τον φυσικό αριθμό

$$a = 3p_1p_2\cdots p_n - 1$$

ο οποίος είναι της μορφής $3k+2$ διότι $a = 3p_1p_2\cdots p_n - 1 = 3p_1p_2\cdots p_n - 3 + 2 = 3(p_1p_2\cdots p_n - 1) + 2$.

Ισχυρισμός: *ο αριθμός a έχει έναν πρώτο διαιρέτη της μορφής $3k+2$.*

Πράγματι: $a > 1$ και άρα ο a έχει έναν πρώτο διαιρέτη p ο οποίος θα έχει μια από τις παρακάτω μορφές: $d = 3k$ ή $d = 3k+1$ ή $d = 3k+2$. Επειδή ο p είναι πρώτος, προφανώς ο p δεν μπορεί να είναι της μορφής $3k$. Αν όλοι οι πρώτοι διαιρέτες του a είναι της μορφής $3k+1$, τότε επειδή από το Θεμελιώδες Θεώρημα της Αριθμητικής κάθε φυσικός αριθμός > 1 είναι ίσος με το γινόμενο (δυνάμεων) των πρώτων διαιρετών του και επειδή προφανώς γινόμενο αριθμών των μορφής $3k+1$ είναι της μορφής $3k+1$, έπεται ότι ο a θα είναι της μορφής $3k+1$ το οποίο είναι άτοπο διότι ο a είναι της μορφής $3k+2$. Άρα τουλάχιστον ένας πρώτος διαιρέτης p του a είναι της μορφής $3k+2$.

Επειδή $p_1, p_2, \cdots, p_n$ είναι όλοι οι πρώτοι της μορφής $3k+2$, έπεται ότι $p = p_i$ για κάποιο $i = 1, 2, \cdots, n$. Τότε επειδή $p \mid a$ και $p \mid 3p_1p_2\cdots p_n$, θα έχουμε ότι $p \mid -1$ το οποίο είναι άτοπο. Άρα το πλήθος των πρώτων αριθμών της μορφής $3k+2$ είναι άπειρο.

(β) Υποθέτουμε ότι υπάρχει πεπερασμένο πλήθος πρώτων της μορφής $4k+3$, και έστω ότι όλοι οι πρώτοι της μορφής $4k+3$ είναι οι $p_1, p_2, \cdots, p_n$. Θεωρούμε τον φυσικό αριθμό

$$a = 4p_1p_2\cdots p_n - 1$$

ο οποίος είναι της μορφής $4k+3$ διότι $a = 4p_1p_2\cdots p_n - 1 = 4p_1p_2\cdots p_n - 4 + 3 = 4(p_1p_2\cdots p_n - 1) + 3$.

Ισχυρισμός: *ο αριθμός a έχει έναν πρώτο διαιρέτη της μορφής $4k+3$.*

Πράγματι: $a > 1$ και άρα ο a έχει έναν πρώτο διαιρέτη p ο οποίος θα έχει μια από τις παρακάτω μορφές: $d = 4k$ ή $d = 4k+1$ ή $d = 4k+2$ ή $d = 4k+3$. Επειδή ο p είναι πρώτος, προφανώς ο p δεν μπορεί να είναι της μορφής $4k$ ή $4k+2$. Αν όλοι οι πρώτοι διαιρέτες του a είναι της μορφής $4k+1$, τότε επειδή από το Θεμελιώδες Θεώρημα της Αριθμητικής κάθε φυσικός αριθμός > 1 είναι ίσος με το γινόμενο (δυνάμεων) των πρώτων διαιρετών του και επειδή προφανώς γινόμενο αριθμών των μορφής $4k+1$ είναι της μορφής $4k+1$, έπεται ότι ο a θα είναι της μορφής $4k+1$ το οποίο είναι άτοπο διότι ο a είναι της μορφής $4k+3$. Άρα τουλάχιστον ένας πρώτος διαιρέτης p του a είναι της μορφής $4k+3$.

Επειδή $p_1, p_2, \cdots, p_n$ είναι όλοι οι πρώτοι της μορφής $4k+3$, έπεται ότι $p = p_i$ για κάποιο $i = 1, 2, \cdots, n$. Τότε επειδή $p \mid a$ και $p \mid 4p_1p_2\cdots p_n$, θα έχουμε ότι $p \mid -1$ το οποίο είναι άτοπο. Άρα το πλήθος των πρώτων αριθμών της μορφής $4k+3$ είναι άπειρο. ■

Άσκηση 19. *Δείξτε ότι για κάθε $n \geq 3$, υπάρχουν άπειροι πρώτοι αριθμοί οι οποίοι* **δεν είναι** *της μορφής $nk+1$.*[5]

Λύση. Υποθέτουμε ότι υπάρχει πεπερασμένο πλήθος πρώτων οι οποίοι δεν είναι της μορφής $nk+1$, και έστω ότι όλοι αυτοί οι πρώτοι είναι οι $p_1, p_2, \cdots, p_m$. Μπορούμε να υποθέσουμε ότι $p_1 = 2$ ο οποίος δεν είναι της μορφής $nk+1$ (αν ήταν θα είχαμε $2 = nk+1$ δηλαδή $nk = 1$ το οποίο είναι άτοπο διότι $n \geq 3$). Θεωρούμε τον φυσικό αριθμό

$$a = np_1p_2\cdots p_m - 1$$

Ισχυρισμός: *ο αριθμός a έχει έναν πρώτο διαιρέτη ο οποίος δεν είναι της μορφής $nk+1$.*

Πράγματι, έχουμε $a \geq n - 1 \geq 2$ και άρα ο a έχει έναν πρώτο διαιρέτη. Αν κάθε πρώτος διαιρέτης του a είναι της μορφής $nk+1$, τότε επειδή από το Θεμελιώδες Θεώρημα της Αριθμητικής κάθε φυσικός αριθμός > 1 είναι ίσος με το γινόμενο (δυνάμεων) των πρώτων διαιρετών του και επειδή

[5] Επομένως υπάρχουν άπειροι πρώτοι οι οποίοι *δεν είναι* της μορφής $3k+1$, $4k+1$, $5k+1$, $\cdots$ (και προφανως, για $n = 2$, υπάρχει μόνον ένας πρώτος αριθμός ο οποίος δεν είναι της μορφής $2k+1$, ο πρώτος 2).

προφανώς γινόμενο αριθμών των μορφής $nk+1$ είναι της μορφής $nk+1$, έπεται ότι ο a θα είναι της μορφής $nk+1$. Όμως ο a δεν μπορεί να είναι της μορφής $nk+1$ διότι αν ήταν θα είχαμε

$$nk+1 = n_1p_2\cdots p_m - 1 \implies n(k-p_1p_2\cdots p_m) = 2 \implies n \mid 2 \implies n \leq 2$$

Αυτό είναι άτοπο διότι από την υπόθεση $n \geq 3$. Άρα πράγματι ο a έχει έναν πρώτο διαιρέτη p ο οποίος δεν είναι της μορφής $nk+1$.

Επειδή $p_1, p_2, \cdots, p_m$ είναι όλοι οι πρώτοι οι οποίοι δεν είναι της μορφής $nk+1$, έπεται ότι $p = p_i$ για κάποιο $i = 1, 2, \cdots, m$. Τότε επειδή $p \mid a$ και $p \mid np_1p_2\cdots p_m$, θα έχουμε ότι $p \mid -1$ το οποίο είναι άτοπο. Άρα το πλήθος των πρώτων αριθμών οι οποίοι δεν είναι της μορφής $nk+1$ είναι άπειρο. ■

- **Συμβολισμός:** Έστω p πρώτος. Αν n είναι ένας φυσικός αριθμός και $k \in \mathbb{N}_0$, τότε θα γράφουμε:

$$p^k \| n \quad \iff \quad p^k \mid n \quad \text{και} \quad p^{k+1} \nmid n$$

δηλαδή p^k είναι η μεγαλύτερη δύναμη του p η οποία διαιρεί τον n, και όπου $k = 0$ αν $p \nmid n$.

Άσκηση 20. *Έστω p πρώτος. Ορίζουμε συνάρτηση*

$$v_p \colon \mathbb{N} \longrightarrow \mathbb{N}_0, \quad v_p(n) = \max\{k \in \mathbb{N}_0 \mid p^k \| n\}$$

Αν $\mathbb{P} = \{p \in \mathbb{N} \mid p : \text{πρώτος}\}$ είναι το σύνολο των πρώτων αριθμών, να δείξετε ότι:

(1) $v_p(n) = 0,\ \forall p \in \mathbb{P} \iff n = 1.$
(2) $v_p(mn) = v_p(m) + v_p(n),\ \forall p \in \mathbb{P}.$
(3) $m \mid n \iff v_p(m) \leq v_p(n),\ \forall p \in \mathbb{P}.$
(4) $v_p(m) = v_p(n),\ p \in \mathbb{P} \iff m = n.$

Λύση. (1) Αν $n = 1$ τότε για κάθε $p \in \mathbb{P}$ έχουμε $v_p(1) = \max\{k \in \mathbb{N}_0 \mid p^k \| 1\} = 0$.
Αντίστροφα αν $v_p(n) = 0,\ \forall p \in \mathbb{P}$, τότε δεν υπάρχει πρώτος που να διαιρεί τον n στη πρωτογενή του ανάλυση, δηλαδή αναγκαστικά $n = 1$.

(2) Χρησιμοποιώντας τη πρωτογενή ανάλυση των αριθμών m και n έχουμε ότι

$$m = p^a q \quad \text{και} \quad n = p^b q'$$

με $(p, q) = 1$ και $(p, q') = 1$. Τότε

$$mn = p^{a+b} qq'$$

και $(p, qq') = 1$ διότι διαφορετικά αν $p \mid qq'$ τότε $p \mid q$ ή $p \mid q'$ που είναι άτοπο. Άρα $\forall p \in \mathbb{P}$ έχουμε

$$v_p(mn) = a + b = v_p(m) + v_p(n)$$

(3) Έστω $m \mid n$, άρα υπάρχει c έτσι ώστε $n = mc$. Τότε από το προηγούμενο ερώτημα έπεται ότι

$$v_p(n) = v_p(mc) = v_p(m) + v_p(c)$$

και άρα $v_p(m) \leq v_p(n)$ για κάθε $\forall p \in \mathbb{P}$.
Αντίστροφα ορίζουμε

$$c = \prod_{p:\text{πρώτος}} p^{v_p(n) - v_p(m)}$$

Τότε $m = nc$ και άρα $m \mid n$.

(4) Έπεται άμεσα από το ερώτημα (3). ■

Άσκηση 21. *Έστω p ένας πρώτος αριθμός και $n, m, a, b \in \mathbb{N}$. Να δειχθούν τα ακόλουθα:*

(1) $p^n \| a \ \ \& \ \ p^m \| b \implies p^{n+m} \| ab.$
(2) $p^n \| a \implies p^{nk} \| a^k.$

(3) $n \neq m \quad \& \quad p^n \| a \quad \& \quad p^m \| b \quad \Longrightarrow \quad p^{\min\{n,m\}} \| (a+b)$.

Λύση. (1) Έστω $p^n \| a$ και $p^m \| b$. Άρα $p^n \mid a$, $p^{n+1} \nmid a$ και $p^m \mid b$, $p^{m+1} \nmid b$. Άρα

$$a = p^n q \quad \text{και} \quad b = p^m r$$

όπου το p δεν εμφανίζεται στη πρωτογενή ανάλυση των αριθμών q και r. Τότε

$$ab = (p^n q)(p^m r) = p^{n+m} qr$$

και άρα $p^{n+m} \mid ab$ και $p^{n+m+1} \nmid ab$ αφού το p δεν διαιρεί το qr. Επομένως $p^{n+m} \| ab$.

(2) Έστω $p^n \| a$, δηλαδή $p^n \mid a$ και $p^{n+1} \nmid a$. Άρα $a = p^n m$ όπου $p \nmid m$. Τότε $p \nmid m^k$ και έχουμε

$$a^k = p^{kn} m^k$$

Συνεπώς $p^{nk} \| a^k$.

(3) Έστω $p^n \| a$ και $p^m \| b$ με $n \neq m$. Έχουμε

$$a = p^n q \quad \text{και} \quad b = p^m r$$

όπου το p δεν εμφανίζεται στη πρωτογενή ανάλυση των αριθμών q και r.

Υποθέτουμε ότι $n = \min\{n, m\}$. Τότε

$$a + b = p^n q + p^m r = p^n (q + p^{m-n} r)$$

Επειδή $p \nmid q$ αλλά $p \mid p^{m-n} r$ έπεται ότι

$$p \nmid (q + p^{m-n} r)$$

Επομένως έχουμε ότι $p^{\min\{n,m\}} \| (a+b)$. ■